qulto
for culture & knowledge

Data Protection Statement

v1.0
17 May 2018

Purpose of the document

Monguz Ltd. produces and distributes custom developments and out-of-the-box software products, and it provides its clients with IT services. The present statement summarizes those solutions, techniques and practices that ensure maximum and ongoing compliance with data protection and management rules in case of the Qulto portfolio, custom developments and IT services.

Definitions

CMS	Integrated Collections Management System
Client	Legal persons contracted with Monguz Ltd. Generally public or higher education institutions, who provide support for their institutional workflow and services with the help of a Qulto product or a custom developed software produced by our company.
User	Natural persons using the software.
Institutional user	Users of the software - librarians, archivists, museologists - who operate the system generally as employees of, and on behalf of the client.
Patron	Users of the software who are registered by the client, and use the services provided by the client. (In short, patrons indicated in this document are researchers, students and contracted partners using services offered by public collections.)
Online user	Users of the public Qulto components and portals, who are not contracted partners of the institutions. They may be either registered or not registered users.
PEAS user	Users of PEAS ERP system: client managers, business partners, colleagues.
Loan data	Data of loan transactions that must include the patron’s unique ID, the loaned document’s or item’s ID, and loan date.
Patron’s card	A physical card or document belonging to a patron, issued for a definite period of time. It indicates the scope

	of the contractual relationship between the institution and the patron.

Data protection areas

Our data protection rules apply in three major areas.

Our major field of operation is software development, within which we focus on product development. Components of the Qulto product family are widely used both in Hungary and abroad by several public collection, higher education and public education institutions. Our software products serve as a tool in our clients' hands to, among others, manage data and provide different services as part of their workflow. We find it crucial to ensure that our software assist our clients in being able to comply with data management and data protection rules to the maximum. These measures include access control, technical realisation of data security, and providing functions necessary for standard data management.

Besides producing Qulto software products, we are offering cloud-based services to our clients to an increasing degree. This solution assumes a high level of trustworthiness since customers delegate the management of all of their data and services to a framework operated by a separate party. In order to perform successful business activity, we are committed to make our infrastructure - including hardware and software elements, and related services - comply with all requirements imposed by data protection and data security.

In the course of our system support activities, we often encounter data that is collected and stored by our clients and that might contain personal information. We control our support activities in a way that we can gaurantee their data is secure with us while being processed.

Data protection and data management in Qulto products

The primary aim of the Qulto software is to support the management of both library, museum, archive registries, repositories and knowledge bases, and related processes, services. Systems using our software store an enormous amount of important, confidential, and personal data, hence regulation of data protection and data management is a crucial issue.

Data protection while using the software

Access control - In our systems, access to the infrastructure and applications is regulated according to roles. User groups are created with such a logic that ensures employees' access only to authorized tasks.

Authentication - All logins are secured with a password that are stored in encrypted format, and encryption is also used while they are being transferred within the network.

Technology - When opting technological elements (database-manager, webserver, etc), we consider security principles, hence protecting our clients' data.

Storing client data - In Qulto products, personal data is handled with extreme care, and sensitive personal data such as bank and credit card data is not stored. Our systems provide the possibility of eliminating user data, in compliance with data protection regulation of institutions.

Data protection policies in Qulto products

In case of all Qulto software, the following directives determine how protection of clients' data belonging to certain groups is implemented. A "User" group includes institutional workers using the system, employees (institutional users), patrons having a contractual relationship with the institutions (readers, researchers, etc), and registered visitors using online services free of charge (online users). The regulation covers the instructions related to protection of users' personal data, respecting their rights, tools, and rules of data management and data storage.

By personal data we mean all kinds of information that is required for the identification of users, including but not exclusively the user's name, personal profile, home or other physical address, e-mail address or other contact details. Information related to services used by patrons, loans, fees and circulation data also fall into the category of personal information. Qulto software process such personal data with confidentiality in all circumstances, in compliance with data protection regulations.

Collecting personal data

Online users

Generally, our websites and institutional portals do not require compulsory registration, there is no need for the visitors' providing personal information in order to have access to the sites. However, certain data must be given when online users initiate active communication or conversation, they would like to use the upload feature, or they wish to use a certain function tied to identification.

Institutional users

In case of institutional users only the data necessary for identification (name, user name and encrypted password) is stored, we do not request and handle further information. Depending on system settings, cataloging, circulation and acquisition logs are created by the applications. The only purpose of stored data is to be able to track when and by whom a certain record was modified. It is important to note that the log feature in our systems is not suitable for monitoring employees, tracking activities, or creating daily performance reports.

Patrons

In fact, being enrolled patrons or archive and museum researchers, clients of public collections have a contractual relationship with the institution: the institutions provide their clients with printed or digital contents, objects, tools, and space either free of charge or for a certain fee, according to mutually agreed, predefined conditions. Patrons are responsible for the usage of services in line with the predefined conditions. For managing financial transactions and possible debates or compensation cases related to services, it is necessary to store data used for patrons' exact identification and communication.

Our software can store the following data: name, date and place of birth, mother's name, ID number, temporary and permanent address, e-mail address. Optionally, higher education institutions may identify their users with the help of student IDs upon the institution's request.

With statistical purposes, the institutions have the possibility to enter other information in the system. Content and nature of such data is not determined by the Qulto software, but defined by the institutions themselves complying with, and based on their own regulations and responsibilities. Our software log patrons' transactions, and store them for a definite period of time determined by the client.

Method of using personal data

Data is stored in the system only until

- it is necessary for providing services and products
- it is involved in a currently active process
- it is useful for the user
- it is necessary for the institution's statistical data service
- it is specified by law (for instance invoices)

Requirements related to our collecting and storing data are defined by our clients. It is our explicit responsibility not to collect, store, serve and use personal information for our own purposes beyond these initially defined requirements. Our software do not use personal information for any other purpose, they do not share it with other systems, and they do not transfer or hand it over to a third party, except for some special, properly and clearly defined cases.

These cases are the following:

- in contentious cases, for institutions cooperating in claim management issues (payment order)
- upon request, we provide information for maintaining institutions in case of schools, higher education institutions or workplaces about unclosed loans and debts of students, university students, and employees

User rights related to personal data

Users are authorized to have access to their personal data stored by the system. They might request the modification or erasure of such data, as well. The online interfaces of our applications offer users the possibility to send their remarks related to their stored data online. All requests on modification or erasure is, according to the preliminary settings, automatically forwarded by the system to the person in charge of data protection issues at the institution who evaluates the request.

Data retention and erasure

Three phases are differentiated in our systems from personal data management point of view:

- Active phase - In the Active phase, there is a contractual relationship or transaction in progress between the institution and the user (institutional user, patron, online user). That is why it is necessary and important in this phase to retain information related to identification, communication, pricing, and unclosed loans.

- Statistical phase - After the active phase the institution might need the above data in order to fulfill its obligation related to statistical reports. In case of such data, exact knowledge and identification of users is neither necessary nor wanted, but the activity itself has relevance from statistical point of view. The Qulto systems offer an anonymization function to prevent individuals' identification.

- Archive phase - When the statistical phase is over, our system offers different archiving and erasure methods to implement physical erasure and archiving of data, the latter of which hinders data recovery.

Data protection and data security in cloud services

It is our aim to serve our clients with such secure and reliable frameworks that are compliant with the data security, data access, and data protection principles. We provide cloud services in cooperation with responsible subcontractors who ensure an infrastructure and system being in compliance with data security and data protection principles, document the system itself and the activities in detail, and possess appropriate quality assurance and certificates.

Data security

Data security is ensured by the following operational activities:

- 7x24 hours monitoring and surveillance that aims to trace and analyze suspicious activities, unusual incidents, and potential risks
- monitoring security information and installing security updates in case of OS and other, third-party software suppliers
- daily backups, checking and storing backups in compliance with storage policy
- regulating network connections and user access

Developing the physical environment

Points to consider when developing the service framework in order to avoid data loss:

Servers are stored in a proper place appointed specifically for this purpose and equipped with

- an uninterruptible power supply (UPS) of appropriate capacity
- air-conditioning ensuring the optimal operating temperature
- an appropriate fire protection system

Physical access monitoring

Entrance to server rooms is restricted to colleagues who need to have access to the hardware. All physical accesses are logged.

Information security provisions

Operation system

Only necessary components are installed in the browser, and all accesses are strictly regulated.

Network security

Firewalls: The servers are protected with firewalls in order to avoid online attacks and client data loss.

Data erasure

In case a client decides to terminate the cooperation with our company and is not willing to use our solutions anymore, data is handed over to the client saved on a data medium. When the previously agreed termination period expires, we erase all client data from all data medium without the possibility of data recovery.

Data protection and data management in system support services

In the frame of our software support service we provide our clients with system support services and error report system.

Data protection in system support

Client support work includes several tasks: debugging, conversion, and so on. In order to carry out these tasks effectively, in most cases access is required to the database, so as to personal information, as well.

We do not

- use for other purposes
- hand over to a third party
- store
- allow unauthorized access in the course of processing to

data that is provided to us by clients

All of our colleagues and subcontractors are bound by professional secrecy, therefore usage restrictions apply to them, as well.

Data management in PEAS

For keeping track of error reports, the PEAS ERP system is used. Most important data (that are used for communication) of clients, business partners and contact persons are documented in this system. In case of individuals these include name, phone number, address, e-mail address, title. Companies’ data include invoicing details in addition. Clients have the opportunity to view their data on the web surface, and may initiate their modification or erasure.